2008 年 5 月 30 日

參考文件

立法會資訊科技及廣播事務委員會

資訊保安

目的

本文件的目的，是向委員會簡述政府及公共機構資訊保安的現況及就最近的資料外泄事故取得的經驗而作出的改善計劃，從而減少將來發生事故的風險。

政府就資訊保安所持的立場

2. 政府非常重視資訊保安和保護內部的資訊及電腦資產。在數碼21資訊科技策略下，建立一個穩妥的環境，是推動資訊及通訊科技在本港發展的重要一環。政府已就資訊保安採取不同措施，以提高社會各界對進行電子交易的信心，藉以促進電子政府及電子商貿的發展。過去數年，我們推行多項與資訊保安有關的計劃，建立公共資訊保安基建，以發展電子商貿和促進資訊及通訊科技在社會上的使用，並已取得實質進展。

3. 政府已制訂和實行一套全面的資訊保安架構，爲保護其管理的資訊資產設立應有的監管和措施。鑒於瞬息萬變的商業

環境、科技發展和社會需求，政府會不斷地更新此架構以緊貼最新的發展。對於最近突然增多的資料外泄事故，政府正注入更多資源加強這架構，以維持資訊保安的最高標準和減低保安事故所帶來的影響。

4. 儘管現況已有很多保護政府資訊資產及市民個人資料的措施，我們明白仍需持續努力，尤其考慮嶄新的威脅和風險，以及保安事故所汲取的經驗。

政府現行保護資訊資產及個人資料的措施

資訊保安的監管

5. 政府制訂了一套全面的資訊保安規例及政策[1]，及頒布給政策局及部門（各局/部門）執行。這些規例、政策及有關的程序及指引是參考國際間良好的作業模式及採用專業資源而制訂，並會不時更新以反映科技發展和保安威脅的轉變。各局/部門須負責整個部門的資訊保安，在運作、組織、管理、技術和程序各方面的考慮下，設立他們的資訊保安架構及作業實務。個別僱員及合約員工須負個人責任，遵從規定的作業實務。

6. 爲監管和執行政府內部的資訊保安，當局於2000年成立資訊保安管理委員會[2]。此外，爲了在行政上支援該委員會，政府更成立資訊科技保安工作小組，負責頒布及監察各局/部門遵行資訊科技保安政策及指引。自2007年5月，中央統籌的保安審

[1]當中包括基準資訊科技保安政策、資訊科技保安指引、保安風險評估及審核指引、資訊保安事故處理指引及軟件資產管理指引。

[2]資訊保安管理委員會核心成員包括保安局及政府資訊科技總監辦公室的高級人員。

計，已開始實施，以確保各局/部門能妥善進行所需的保安風險評估及檢討。

(i) 政府的資訊保安需求

7. 在資料保護方面，《保安規例》有明確要求限制政府把持有的資料作出保安分類及處理。在很多情況下，個人資料是被分類爲 "限閱" 或以上。每一個政府人員對於受限制資料（包括載有個人資料的文件）的保安都應負上個人責任。此外，《保安規例》還有特定的章節涵蓋資訊系統及有關儲存、處理和傳送資訊的規例。

8. 政府資訊科技總監辦公室已制訂了一套指引，建議各局/部門資訊保安的執行措施。這些指引所涵蓋的一些課題列舉於本文附件 1。軟件資產管理指引，尤其針對妥善管理及使用電腦軟件。另外，正確使用互聯網指引已發給所有政府人員，協助他們使用互聯網。當各局/部門進行系統發展項目時，資訊科技總監辦公室也會要求及協助他們落實私隱影響評估和保安影響評估。

(ii) 政策局／部門

9. 各局/部門須參照基準資訊科技保安政策來制訂其部門資訊科技保安政策及執行必需的資訊保安管理和保護措施[3]，包括部門資訊保安通告、指示和程序，以協調及管理事務應用系

[3]包括委任高級人員擔任部門電子事務統籌人員、部門資訊科技保安主任、網絡管理員及資訊保安事故應變小組。部門資訊科技保安主任負責整個部門的資訊保安管理與運作。資訊保安事故應變小組協調日常關於資訊保安事故的滙報及應變。

統、資訊科技資源、資訊保安措施及事故應變處理。

10. 在保護部門的資訊系統及電腦設施方面，部門須執行必要的措施確保商務交易和資訊的完整性[4]及最少每兩年一次替其資訊系統、網絡及服務進行保安風險評估。另外，政府資訊科技總監辦公室已提供一份自我評估表格給各局/部門每年填報，以了解他們保安改善情況。

11. 當發生資訊保安事故時，各局/部門須根據事故的嚴重性，向政府資訊保安事故應變辦事處作出之匯報。

12. 各局/部門須確保員工接受足夠及適當的資訊保安培訓，及應傳閱中央發出的規例、政策、指引、程序、通告及警報給所有工作人員包括外判員工[5]，以保持員工在處理資料時擁有最高的認知、知識和技能。

(iii) 政府員工

13. 所有政府員工需要遵從就資訊保安及個人資料保護的相關規例及指示。資訊保安是每一個員工的個人責任，政府員工在處理政府的受限制資料(包括載有個人資料的文件)時，要遵從保安要求。他們有責任認識、明白、遵從和盡可能執行所有可行及可用的保安措施，以及盡力防止未被授權的人閱覽他們的電腦和工作站。

[4]這些措施包括實體保安、存取控制程序及電子認證措施。
[5]此外，各局/部門也須定期再傳閱該批文件以提醒員工。

(iv)　公共機構

14.　各局/部門在規管轄下的公共機構時，會參考政府的保安規例和政策以作出相應的規管或行政安排。爲了監察公共機構的正常運作，部門與其轄下的公共機構需要協商資訊資產的保護，以防止發生任何資訊保安事故，影響公共服務的提供。各局/部門須與公共機構協調資訊保安計劃及執行有關的措施，確保必須的保護措施及事故應變能力有效地執行及運作。我們建議公共機構，制定他們的資訊保安政策、項目計劃及執行措施時，可採納或按需要修訂相關政府資訊保安政策、指引及技術文件內容。最重要是公共機構對網上的保安威脅須保持警惕，還須強化他們的保安狀況，以保護其電腦資產和所持有關市民的資料。

<u>保護措施的執行</u>

(i)　技術措施

15.　政府採用「防護、偵察、反應及恢復」的原則，以確保業務交易和資訊的完整性。爲防範不同種類的網上攻擊[6]，我們執行了必需的措施，包括採用各種最新科技應用在各種服務層面或個別資訊科技項目[7]上。此外，政府資訊科技總監辦公室除了爲某些主要的資訊科技項目建議資訊保安要求、標準、設計及方案，還協助各局/部門選購所需的軟件及資訊科技保安專業服務。爲了方便各局/部門處理有關資訊保安事宜及採購外間資

[6]包括電腦蠕蟲和病毒、黑客入侵、濫發訊息及電腦罪行等不同的威脅。

[7]這些措施包括防火牆、抗禦電腦病毒軟件、入侵偵察系統及其他防禦機制，以監測、偵察和堵截政府電腦網絡及系統可能受到的入侵，並會定時安裝最新的修補及糾正程式。

源，政府資訊科技總監辦公室已就資訊保安專業服務制訂常備承辦協議。

16. 爲了保護受限制/個人資料或服務免被外泄，多種服務層面與部門資訊科技系統和網絡已實施合適的登入程序和接達授權。爲了更強化資料存取的控制，政府資訊科技總監辦公室已於2004年推行風險評估和電子認證架構，以確保各局/部門在推行他們的電子政府服務時已執行風險評估和合適的保護措施。於2007年12月，我們已頒布「統一身份管理架構」，確保市民可在最新推出的電子政府服務統一的客戶界面和賬戶管理程序去辦理客戶登記、服務註冊和客戶認證。此架構目的在爲大衆提供方便與保護資訊資產之間取得平衡。無論如何，對技術性和程序上的措施進行定期的保安檢討和審計可確保他們能夠配合科技的發展、業界的最佳作業模式以及系統、網絡或機構環境的改變。

(ii) 遵從保安要求

17. 自2007年5月，政府已執行一個由中央管理的保安審計，定期替各局/部門確實其遵從保安要求和妥善執行已識別的改善事宜。這個初部系列的保安審計將於2009年5月完成審查所有部門。

(iii) 員工對資訊保安的認知與教育

18. 政府非常關注員工在資訊保安方面的培訓，也承諾使員工能獲得資訊保安的知識和技巧。爲了在管理和運作層面加強員工對資訊保安及相關最佳作業模式的認識，政府資訊科技總監辦

公室已製備多份策劃、管理及技術方面的保安指引，以供各局/部門參考，並透過研討會、專題網頁及參考指南向各員工傳達。政府會因應新的保安威脅及相關的預防措施，不時更新這些指引。此外，我們並設立完善的溝通網絡，向全政府發放保安威脅及警告的相關資訊。政府資訊科技總監辦公室已定期向各局/部門發出有關資訊保安的催辦便箋，提醒各員工留意軟件漏洞和保安威脅，並就保護資訊資產提供指引。

19. 我們已聯同多個局/部門舉辦資訊保安有關的研討會及培訓課程，範疇包括資料保護、事故應變處理、網絡應用系統保安、資訊科技外判保安等。此外，我們與公務員事務局一般職系處合作，特別爲行政主任職系舉辦了"政府資訊保安"課程，以加強這些人員特定的知識和技能，應付日常部門運作需要。我們製作了兩個有關"資料保護"的網上課程。政府人員可透過公務員培訓處的網上電子學習平台"公務員易學網"，修讀這兩個課程。

20. 政府資訊科技總監辦公室利用多種資訊發放渠道，向政府人員及市民推廣和教育資訊保安的專題資訊。這些渠道包括網站[8]、宣傳單張、小冊子、電台和電視廣播。於 2007 年，我們派發「保護你的電腦資料」單張[9]，內載「確保手提儲存設備安全」及「爲敏感資料加密」的主要信息。爲引導用戶正確使用互聯網的服務與突顯有關法例，我們亦已製作"正確使用互聯

[8]政府熱衷分享其資訊保安的知識和經驗給市民大眾，使公眾更支持建立健康的數碼社區。我們不時製作有關資訊保安的技術指引及參考資料，並把資料截於一站式資訊保安入門網站（網址：www.infosec.gov.hk），以供市民閱覽。

[9]有關網站索引頁及單張的內容，請參閱附件 2。

網的守則"[10]，以供政府員工和市民大眾參考。

(iv)　事故應變處理機制

21.　如遇保安事故，各局/部門會立即展開初步調查，並視乎事故嚴重程度(例如事故會影響公共服務或政府)向政府資訊保安事故應變辦事處匯報。一般而言，機密及個人資料的泄漏均需要作出滙報。政府資訊保安事故應變辦事處負責協調和支援各局/部門應付有關保安的資訊保安事故。

從最近發生的保安事故汲取經驗

22.　自2008年4月中起，政府及公共機構發生多宗保安事故，涉及個人資料泄漏，引起市民的關注（有關最近發生的保安事故摘要，請參閱附件3）。其中一些事件的調查仍在進行，初步結果顯示，大部分事件是由於員工對現有的資訊保安規例、政策及指引(特別是在使用便攜式電子裝置及文件共享軟件方面)的認識及／或警覺不足所致。此外，員工對資料保護和在辦公室以外的地方（例如家中）處理公務文件的額外潛在風險的有關認知，亦非常重要。

23.　在現今的電腦使用環境下，新出現的保安威脅正不斷挑戰終端用戶的裝置（如個人電腦、個人數碼助理和多功能流動電話等消費者裝置、以及 USB 快閃裝置、記憶卡、外置磁碟等便攜式電子儲存裝置）所儲存之資料保密性。此外，廣泛應用

[10]指引特別提及用戶不應發行、刊載、傳輸、連結、發放或訂閱任何含有欺騙、淫穢、煽動、冒犯、誹謗、威脅或不法的資料、惡意程式碼或材料。

和依賴互聯網這個平台作商業、工作、學習、消閒等活動也會帶來網上保安威脅。這些威脅有小部分是不經意或由於人爲錯誤產生，其餘很多是含有惡意動機，包括不正當的獲利、作弄和破壞、以及嘗試盜竊身份和其他欺騙行爲。

24. 就最近發生的保安事故，我們已加強了一些保護電子資料的措施。這些措施包括：增強所有員工對資訊保安要求的意識及確保他們明白如何遵守規例；確保他們能具備所需的軟件和基礎建設，以遵守規例和減少資料儲存於便攜式裝置的機會；加強管理機制，確保政府和公共機構遵守規例，提供給機構所需的意見和協助；計劃長期技術性改善措施使員工更易遵守規例，以及政府更容易防止和偵察違反規例的事故。

政府的資訊保安強化計劃

25. 政府在汲取這些事件的經驗後，已迅速提醒所有員工，必須遵守有關保護資訊系統和受限制/個人資料的資訊保安要求。我們已引入新的要求及建議以減低一些涉及便攜式電子儲存裝置的事故所帶來的風險。我們亦已發出更多的技術資訊和指引，加深員工對有關規例、程序和資訊科技方案的認識。最近發生保安事故的有關局/部門已即時採取改善行動，詳情請參閱附件 3。其他局/部門亦已更新他們的內部通告和舉辦緊急簡報會，以確定員工注意及遵從這些催辦便箋和附加指引。此外，政府已即時採取一套改善措施，以減低保安風險及因違反規例可能導致的後果。此強化計劃會在未來數月推出並涵蓋以下四個範疇，包括加深員工對資訊保安的認知和教育、技術及程序

措施、遵從保安規定檢查，以及檢討保安規例、政策及指引。

(i)　　員工的認知與教育

26.　資訊保安的關鍵在於人們，因爲他們擔任的角色可以是資料的擁有人、管理人、中介人或用家。員工的認知、教育和培訓對加強政府資訊保安的整體策略均是十分重要的。

(a)　　加強員工遵守規例的催辦便箋及指引

27.　爲了改善資料保護得以遵守，政府資訊科技總監辦公室已於 2008 年 5 月 2 日向各局/部門發出催辦便箋及指引，提醒他們保護資訊系統及資料，尤其在安全及正確使用便攜式電子裝置及共用檔案技術時須注意的事項。通告亦特別提出，在沒有事先獲部門批准前，禁止員工把未經授權的應用軟件上載於政府的資訊系統，或把未經授權的資訊系統設備接駁至政府的資訊系統。此外，亦爲提供其他有關資料保護技術方案，包括資料加密，存取控制、資產管理及實體儲存，以便各局/部門執行必須的改善措施。

28.　政府於 2008 年 5 月 8 日向全體公務員發出另一份通告，再次提醒他們注意相關規例及個人資料（私隱）條例的要求，並建議遵行的實際方法。此外，各局/部門須確保員工只限於在「有需要知道」的原則下才可獲取資料。這通告亦加入了新的規定，包括當需要儲存個人或受限制資料於便攜式電子裝置前，必須獲事先授權，並只可儲存最少量的資料，以及使用安全的儲存媒體。儘管如此，各局/部門仍須發放告示和催辦便

箋供員工傳閱，以及爲員工提供內部培訓和協助，使他們能遵從這些規定。

(b) *加強與員工的溝通*

29. 政府資訊科技總監辦公室及保安局在公務員事務局的支援下，將會與部門資訊科技保安主任緊密合作，設計一套員工溝通項目，旨在使政府人員建立和維繫對資訊保安的高度認知和遵從實務守則的知識，以及保護敏感和個人資料的態度和承擔。這個項目將於 2008 年 9 月開始分階段推行。

30. 這個項目將設計及製作包括一套全新資料單張及海報，並於2008年9月向員工推廣有關安全使用及保護便攜式電子裝置的知識。另外，我們也準備於 2008 年 8 月開始於政府內聯網及《公務員通訊》出版以資訊科技保安爲題的文章，以增加政府人員對資訊保安的認識。

(c) *員工培訓*

31. 政府資訊科技總監辦公室已安排在 2008 年開始，在一般職系處爲新招聘的行政主任所辦的入職課程加入資訊保安的簡介。這些新入職人員會稍後被委派當部門資訊科技保安主任或協助管理整個局/部門保安事宜。在部門層面而言，各局/部門會加強管理、前線和支援員工的培訓，包括把資訊保安課題加入他們的員工入職課程及複修研討會。政府資訊科技總監辦公室正安排資訊保安研討會及培訓課程，內容包含有關使用便攜式

電子裝置及保護個人資料的課題，同時會加強推廣使用資訊科技的道德標準和處理受限制/個人資料的正確方法。

(ii)　技術及程序措施

32.　各局/部門正執行有關在便攜式電子裝置儲存個人或受限制資料在技術及程序方面的新規定。我們亦要求各局/部門必須在容易使用和存取控制方面取得平衡，並善用應用軟件及電腦設備的保安功能，以提升其資訊系統、網絡及服務的保安狀況。從最近的保安事故當中，在辦公室以外的地方（例如在家裏）工作是一個明顯的風險來源，所以我們也會協助各局/部門在運作上是有需要的時候，能讓其員工可在辦公室以外的地方（例如在家裏）工作。

33.　就長遠而言，我們正開發一個以更嚴格的方法來推行電子資訊管理的策略，確保電子資訊的產生、儲存、檢索、使用、用以作出決定、出版、搜尋及存檔等方面都受到適當的管理。這個方向包括透過科技應用，不但便利個別人仕確保敏感資料的安全，亦相對地減低因不小心、疏忽或惡意破壞而引致資料外泄的風險。同時，也會提高知識分享、加強合作，以及減少在管理文件紀錄上的成本和對環境帶來的影響。這個基建須數年時間才能全面地在整個政府中落實。

(iii)　加強管理安排以確保規例得以遵行，以及向各政策局及部門、公共機構和非政府機構提供建議及支援

34. 在中央統籌的保安審計中，政府資訊科技總監辦公室會加強關注保護及處理受限制/個人資料，和使用便攜式電子裝置的程序。已完成保安審計的各局/部門會被要求提供補充資料以確定他們已遵行有關的規定，否則須提供工作計劃，改善所有隨後確認的弱點。我們亦會檢討有否其他可以採用的管理步驟，以確保各局/部門、公共機構及提供公共服務的非政府機構，遵行相關的保安政策及作業模式。

35. 政府資訊科技總監辦公室將會繼續透過各局/部門的協調，對其轄下的公共機構及非政府機構提供有關資訊保安的建議，例如，提醒各規管機構檢視是否需要有更嚴緊的規例，從而改善其轄下受規管行業的資訊保安狀況。我們亦會繼續提醒各局/部門向這些機構提供政府內部廣泛採用的保安規例、政策及指引以作參考，從而收緊其保安制度。我們更會透過各局/部門，邀請其轄下的公共機構出席適合的講座及研討會，並會檢視向這些機構提供其他協助，藉以加強其資訊保安的作業模式。

(iv) 檢討資訊保安規例、政策及指引

36. 政府已設立機制，定期檢視及修訂資訊保安管理架構以便各局/部門遵守，以及確保支援措施能夠緊貼日新月異的科技發展、國際間/業界良好作業模式及嶄新的保安威脅。在這方面，政府資訊科技總監辦公室及保安局擔當主導角色，但有需要時，其他行政及執法機構亦會參予。上次檢討工作已於2006年年中完成。政府資訊科技總監辦公室已計劃於2008年下半年度展開新一輪檢討工作。我們會考慮從近日發生的保安事故所得到的經

驗，例如要求滙報所有涉及遺失個人資料的事件，並採取適當的措施藉以減低濫用遺失的資料的機會。在展開全面的檢討前，政府會成立一個工作小組，成員來自政府資訊科技總監辦公室、保安局及警方的代表，盡快審議現行規例及政策，當中特別注重個人資料的保護。預計檢討工作會於2008年9月底前完成。

(v)　公衆的資訊保安

37.　政府已採取措施推廣並教育公衆對正確使用互聯網的認知。我們會與資訊科技界合作在有關的指引內，加入一些個案例子，並加強對企業(尤其中小企)其他推廣活動。此外，我們會繼續加強「資訊安全網」(INFOSEC 網站)的內容，同時也會透過我們的學校訪問計劃，增強兒童及青少年的認知，尤其在使用互聯網服務時應有的道德標準。

未來路向

38.　政府有決心教育及協助所有員工遵守資訊保安規例，以確保政府及市民的受限制/個人資料得到最大程度的保障。

徵詢意見

39. 請委員察悉本文報道的內容。

商務及經濟發展局

政府資訊科技總監辦公室

2008 年**5**月

附件 **1**

政府資訊科技總監辦公室

基準資訊科技保安政策

[S17]

第 3.0 版

二零零六年五月
香港特別行政區政府

目錄

政府資訊科技總監辦公室

資訊科技保安指引

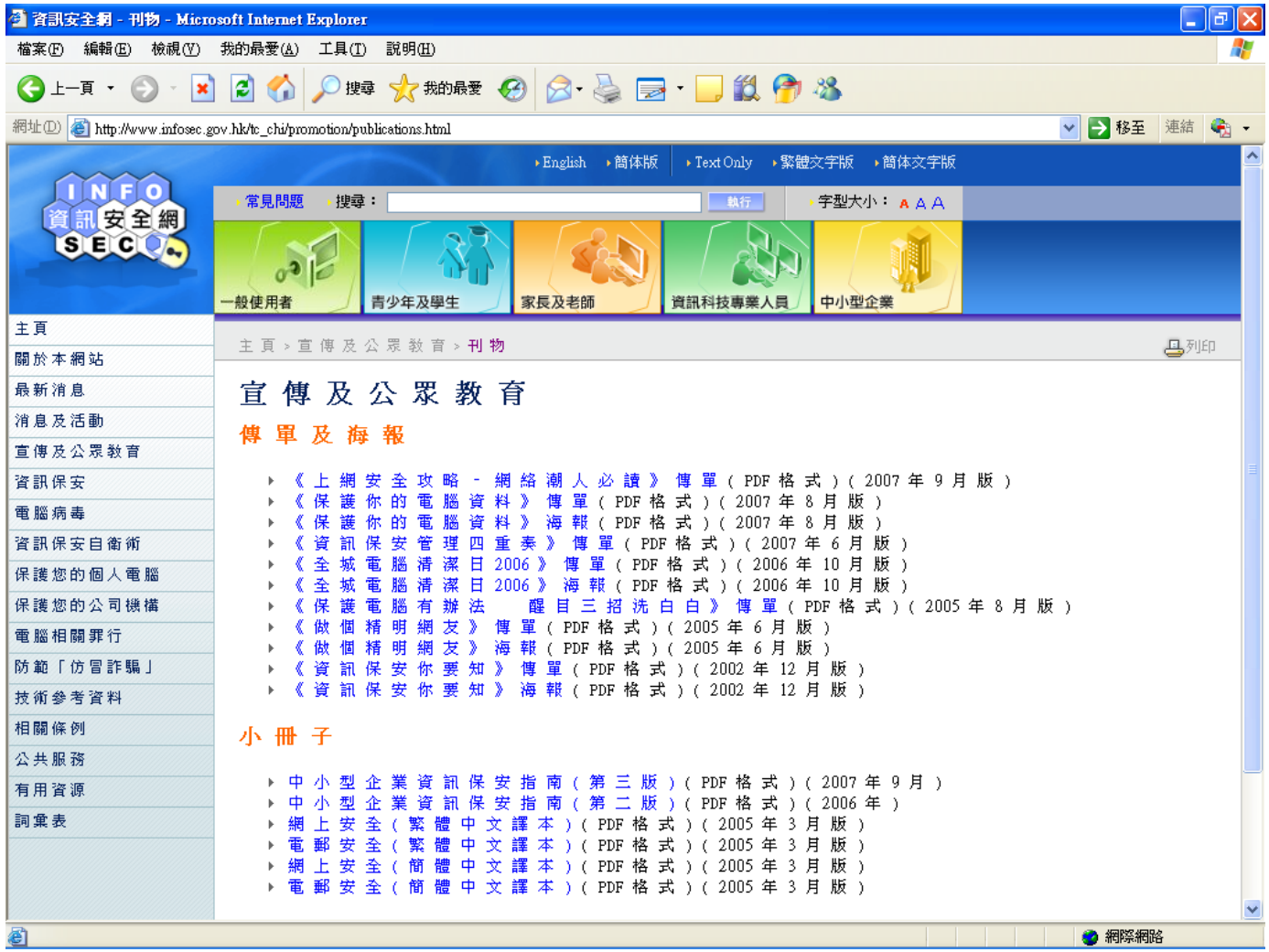
[G3]

第 5.0 版

二零零六年五月
香港特別行政區政府

目錄

附件 2


資訊安全網 - 刊物 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://www.infosec.gov.hk/tc_chi/promotion/publications.html
移至 連結
English 簡体版 Text Only 繁體文字版 簡体文字版
常見問題 搜尋： 執行 字型大小： A A A
一般使用者 青少年及學生 家長及老師 資訊科技專業人員 中小型企業
主頁
關於本網站
最新消息
消息及活動
宣傳及公眾教育
資訊保安
電腦病毒
資訊保安自衛術
保護您的個人電腦
保護您的公司機構
電腦相關罪行
防範「仿冒詐騙」
技術參考資料
相關條例
公共服務
有用資源
詞彙表
主頁 > 宣傳及公眾教育 > 刊物
列印
宣傳及公眾教育
傳單及海報
《上網安全攻略 - 網絡潮人必讀》傳單 (PDF 格式) (2007 年 9 月 版)
《保護你的電腦資料》傳單 (PDF 格式) (2007 年 8 月 版)
《保護你的電腦資料》海報 (PDF 格式) (2007 年 8 月 版)
《資訊保安管理四重奏》傳單 (PDF 格式) (2007 年 6 月 版)
《全城電腦清潔日 2006》傳單 (PDF 格式) (2006 年 10 月 版)
《全城電腦清潔日 2006》海報 (PDF 格式) (2006 年 10 月 版)
《保護電腦有辦法 醒目三招洗白白》傳單 (PDF 格式) (2005 年 8 月 版)
《做個精明網友》傳單 (PDF 格式) (2005 年 6 月 版)
《做個精明網友》海報 (PDF 格式) (2005 年 6 月 版)
《資訊保安你要知》傳單 (PDF 格式) (2002 年 12 月 版)
《資訊保安你要知》海報 (PDF 格式) (2002 年 12 月 版)
小冊子
中小型企業資訊保安指南 (第三版) (PDF 格式) (2007 年 9 月)
中小型企業資訊保安指南 (第二版) (PDF 格式) (2006 年)
網上安全 (繁體中文譯本) (PDF 格式) (2005 年 3 月 版)
電郵安全 (繁體中文譯本) (PDF 格式) (2005 年 3 月 版)
網上安全 (簡體中文譯本) (PDF 格式) (2005 年 3 月 版)
電郵安全 (簡體中文譯本) (PDF 格式) (2005 年 3 月 版)
網際網路


保護你的電腦資料
警告
如何保護你的電腦資料？
電郵
INFO
資訊安全網
SEC
詳情請瀏覽「資訊安全網」：
www.infosec.gov.hk
如果你已做齊以下各項保安措施，
你可算是精明的電腦用家。

附件 3 – 事故摘要

事故 1

事故簡述

屯門兒童體能智力測驗中心一位醫生在其辦公室兼診症室遺失了一枚便攜式儲存裝置。

該名醫生向上司報告此事。服務主管於 2008 年 4 月 22 日向警方報案。衞生署總部其後獲告知有關事件。衞生署於 2008 年 4 月 24 日，致函受影響的兒童及其家人，知會他們這宗事件，並向他們致歉。2008 年 4 月 25 日，個人私隱專員獲告知此事。署方亦於同日召開記者招待會，公開道歉及公布跟進行動。

此外，亦設立電話熱線，接聽電話查詢。

影響

遺失了的便攜式儲存裝置內儲存了工作檔案，當中包括可辨別個人身份的服務使用者資料。個人資料有可能外泄至陌生人手上。

調查結果

事故仍在調查中。

已採取的糾正行動

衞生署已更新有關使用電腦及資訊科技系統可抽離媒體的常務通告，提醒員工除非情況特殊，並已獲得服務單位主管批准，否則不得把可識別身份的個人資料，儲存於可抽離儲存媒體內，或以任何方式傳離衞生署。根據上述情況如需要儲存個人資料，這些資料在儲存時必須加密，並應盡量將相關資料的儲存及傳送減至最少，能應付運作需要便可。使用完畢後，應立即刪除便攜式電子裝置內的資料。

跟進事項

衞生署已建議受事件影響的兒童及其家人保持警覺，如有可疑人物接觸他們，便應向警方報告。此外，他們也獲通知，由於醫療記錄的正本完整無損，因此服務使用者的治療安排不會受到任何影響。

事故 2

事故簡述

公務員事務局在報告中指出，於 2008 年 4 月 23 日遺失了一枚便攜式儲存裝置，內有兩宗紀律研訊資料，當中涉及 25 名在職公務員的姓名及職銜。

局方已向警方報案，以及主動向個人私隱專員公署報告，並向有關的25名公務員致歉。

影響

遺失的便攜式儲存裝置涉及25名在職公務員的姓名及職銜，並沒有公衆的個人資料。

調查結果

公務員事務局已就事件進行調查;並已告誡遺失此便攜式儲存裝置的人員。

已採取的糾正行動

局方已採取行動，檢討對使用和存放載有個人或受限制資料的便攜式儲存裝置的保安措施，以及經訓示及更新內部指引提醒員工時刻遵守有關的指引／規例。

局方已加強保安措施，提醒員工不可使用便攜式儲存裝置下載、儲存或傳送受限制資料。如"確有需要"，員工應事先取得批准及只可使用由局方提供和備有適當防護功能的裝置。局方亦指示員工，在任何情況下不可把受限制資料帶回家中。如有需要，局方可提供保密網絡，備有加密及認證功能的虛擬專用網絡(VPN)筆記簿型電腦，供員工使用。

事故 3

事故簡述

在2008年5月7日，入境事務處（入境處）發現透過一款檔案分享軟件，可在互聯網上搜尋到該處的一些機密資料。

影響

有關電腦軟件的搜尋器可在互聯網上搜尋到一些入境處的機密資料。

調查結果

調查顯示事件涉及一位新入職的入境事務主任，他在本年三月剛完成入職訓練，並調派到管制站工作。爲熟習該管制站的日常運作及本身工作，他向兩位較資深同事借閱文件，存入便攜式儲存裝置，並將副本儲存於家中的電腦用作參考。懷疑此舉引致資料外泄。

已採取的糾正行動

雖然資料是透過有關職員在家中的個人電腦外泄，入境處亦馬上主動檢查部門內所有的電腦終端機，確保沒有安裝未獲授權下載的電腦軟件。處方同時立即派員到該名職員家中，清除儲存在該電腦內的所有有關資料、移除相關的電腦軟件及重新將電腦硬碟格式化。該處並檢查其餘兩名職員的電腦，以確保沒有儲存同類的資料。

處方已即時訓示所有職員，提醒他們遵守有關處理官方文件和保護個人資料的指引、規例及指示。雖然事件起因涉及個別職員在處理資料的保安意識不足，入境處會繼續加強職員對處理個人及機密資料的警覺性。